Resilience Benchmarking Project

Discussion Paper
December 2005

FSA

HM TREASURY

THE BANK OF ENGLAND

Contents

Foreword by Callum McCarthy

Chairman, Financial Services Authority

The Resilience Benchmarking Project has been a major undertaking by the Tripartite Authorities in partnership with the key participants in the UK financial sector. Thus it has been very much a joint effort. The project aspired to address three main questions: how resilient would the UK financial system be if faced with major operational disruption; how quickly could it recover; and what needs to be done to further enhance resilience? The main findings of the project are set out in this Discussion Paper.

It is encouraging that the project has established that the core parts of the financial system appear to be highly resilient, particularly in respect of their IT arrangements. This has led us to our central conclusion that we do not at this stage need to become more prescriptive in our regulatory approach to business continuity management.

Nonetheless, a number of aspects of business continuity planning have been identified as in need of further strengthening. This Discussion Paper outlines those areas for improvement. In particular we are concerned that firms are too inward-looking in respect of their testing and planning arrangements, that more could be done to increase transparency of information between firms and their critical suppliers, and that crisis management arrangements need to be more realistic. This paper suggests how we might, collectively, deliver the necessary enhancements to resilience.

The Tripartite Authorities would welcome your engagement with and comments on the findings of the project and the proposals we have made for strengthening the ability of the financial sector to respond robustly to major operational disruption.

1 Executive summary

1.1 Introduction

At the Business Continuity Roundtable Conference in July 2004, Callum McCarthy, Chairman of the FSA, announced that the *Tripartite Authorities* (FSA, Bank of England and HM Treasury) had launched an ambitious project to assess how the UK financial services sector would be able to cope in the event of *major operational disruption* (e.g. terrorist attacks, natural disasters) and how quickly it could recover afterwards. This paper sets out our headline findings.

We constructed the project to answer the following questions:

- How *resilient* is the UK financial sector?
- How quickly can the sector recover from *major operational disruption*?
- Do firms plan and prepare effectively?
- Are there any concentrations or *dependencies* that could be potential areas of vulnerability?
- What action is needed to improve the *resilience* or recovery capability of the sector?

Given the scale and complexity of the UK financial services sector, we decided that we needed a sophisticated data capture and diagnostic tool to help us to collect, validate, and analyse the data consistently. So we designed a detailed online questionnaire using a proprietary benchmarking system. In addition, we made follow-up visits to a sample of firms. As a result, we have a high level of confidence in the data's reliability. Inevitably, while answering lots of questions, an exercise of this kind raises many more, which we will take forward as part of our follow-up work.

Over 60 of the UK's most significant firms and *financial infrastructure providers* volunteered to take part in the project, answering around 1,000 questions each. This was a substantive exercise in which all participants invested considerable time and resources over several months. The project enjoyed this high level of support and engagement from the industry because participants had a strong appetite for information on how they compared to their peers and what constituted sound practice. To this end, we worked closely with a cross-section of participants who acted as an Industry Support Group to help us to design, build, and test our online questionnaire.

Participant firms are now benefiting from the information emanating from the project. For the first time they have detailed individual benchmarking reports which show how they compare to their peers, highlighting areas of relative strength and weakness. We also believe that the findings are applicable more widely and so this discussion paper sets out the headline results and seeks your feedback on our proposals. We would welcome your comments by end March 2006 and we aim to issue a feedback statement by end May 2006.

The exercise should be seen in the context of the wider programme of work being co-ordinated by the Cabinet Office's Civil Contingencies Secretariat. This programme has recently produced guidance on planning assumptions (http://www.fsc.gov.uk/secure/section.asp?catid=142&docid=1049) which describes the type and scale of events that the financial sector should be planning for.

Please address your comments to:

Kathryn Wakeman, Financial Stability Sector 14SE21G
Financial Services Authority
25 The North Colonnade
Canary Wharf, London E14 5HS
Email: resilience.benchmarkingproject@fsa.gov.uk

1.2 Overall assessment

As far as we are aware, this has been the most comprehensive study of financial sector *resilience* and recovery arrangements ever undertaken. It gives us a very valuable picture of the overall business continuity preparedness of the UK financial sector, in particular as it relates to the core market and financial infrastructure functionality (such as *wholesale payments*, *trade clearing*, and *settlement*) on which the sector as a whole depends[1]. Major disruption of this core functionality would be likely to have effects across the entire financial system. By strengthening weak links and reducing vulnerabilities, not only do

1 For simplicity, entities which contribute to this core functionality are referred to throughout this report as *core firms* and *financial infrastructure providers*.

individual organisations become more *resilient* but they also become better able to act as shock absorbers for the system generally.

The results indicate that *core firms* and *financial infrastructure providers* have highly *resilient IT* systems and can recover critical functions rapidly following *major operational disruption*. Their preparedness stands the sector as a whole in good stead in terms of its overall level of *resilience* and recovery capability.

There are, however, several areas where there is scope for firms to improve their planning and preparation. In particular, the sector would benefit by progressing from a strong but heavily IT-focused disaster recovery approach towards the adoption of more rounded business continuity principles. For example, firms can strengthen their arrangements by being more outward-looking in their approach, collaborating with key third parties to bring about more co-ordinated planning, testing and risk mitigation. This will enable them to base their plans on fact rather than assumption and improve the market's collective ability to recover in the event of a disruption. Firms also need to strengthen their *crisis management arrangements,* particularly as they relate to staff.

The project has also helped us to understand more clearly what the key issues are in relation to concentrations and *dependencies*. The results confirm that the financial system is heavily dependent on IT but that IT arrangements are very *resilient*. The project has also allowed us to map geographical locations of primary and *recovery sites* for critical functions. This has confirmed that there is a high degree of concentration of *critical business functions* in and around London. As part of our follow-up work to the project, we need to understand more clearly how firms can mitigate this risk, for example by being able to switch business to offices with a low likelihood of concurrent disruption. The data also confirms a high degree of reliance on *financial infrastructure providers*, on British Telecom and on *recovery service providers* for back-up workspace. These concentrations are not unexpected but firms and providers could do more to increase transparency over information and co-ordinate more closely on planning and testing.

The benchmarking results for individual firms indicate significant variations in business continuity standards between participants. Several participants have described the exercise as a 'wake up call' in terms of improving business continuity teams' understanding of their firms' *critical business functions*. This is a welcome development but highlights that firms need to do more to ensure that business continuity staff are sufficiently aware of the business functions they are supporting. Almost all participant firms have already indicated that they are planning to make changes to their business continuity arrangements as a result of what they have learned from the project.

1.3 Proposals

The key findings section below sets out the headline results in more detail, including our proposed regulatory and oversight response. In summary, the results do not suggest at this stage that we need to become more prescriptive on *business continuity management*, and so we do not intend to make any new rules or guidance as a result of this project. We will, however, need to keep this under review as we monitor the market's progress in increasing its *resilience*. That said, we recognise that there is a strong appetite across the market for more information on what constitutes sound practice for *business continuity management*. With this in mind, the proposals outlined in this paper include issuing a detailed matrix of observed sound practice and publishing informal targets for the recovery of *wholesale payments*, *trade clearing* and *settlement* by *core firms* and *financial infrastructure providers*.

The project has provided the *Tripartite Authorities* with a yardstick by which to measure progress and a sound factual basis from which to work. The *Tripartite Authorities* intend to conduct follow-up work emanating from the project in a co-ordinated way through a new project. As well as the sound practice guide, this new project will include: following up specific concerns in relation to individual participants; delving more deeply into how firms mitigate geographical concentration; and offering the benchmarking tool to a wider group of firms. The follow up project will start in the new year and will be one of the main strands of work for the Tripartite next year. We will also take into account our findings when planning next year's Market-Wide Exercise, which is a good opportunity to strengthen co-ordinated testing across the financial sector.

Many of the action points we are proposing for firms would also benefit from a co-ordinated approach. For example, existing industry groups (or new focus groups) could take forward some of the findings such as improving transparency of information or helping to promote sound practice. We will act as a catalyst to help set these groups in train.

The following section sets out a summary of our key findings. Throughout this document we have used the word "firm" in the generic sense, to mean all the organisations that participated in this exercise including *financial infrastructure providers*. Words that are shown in italics indicate defined terms which have a specific meaning within the context of this paper. Definitions are provided in the Glossary of Terms at Annex C.

1.4 Summary of key findings and recommendations

How resilient is the UK financial services sector?

The results indicate that individual participants have highly *resilient* IT systems, in particular the *core firms* and *financial infrastructure providers*, where three quarters of them replicate all their transactions across dual, fully staffed sites. This is encouraging but there is scope for firms to collaborate more closely with third parties and so strengthen the collective *resilience* of the system. Our findings and recommendations relating to *resilience* are set out in more detail in Chapter 2, but in summary, they fall into four main categories:

a) Taking more account of key interdependencies during planning and testing. For example, firms could co-ordinate more closely with key third parties such as suppliers, counterparties and emergency services so that they better understand how these will behave during *major operational disruption* and in turn how their actions may affect the firm;

b) Mitigating geographical concentration risk, particularly if this is coupled with reliance on distinct labour pools, transport systems, etc;

c) There also needs to be more transparency over sharing of information between firms and their critical suppliers. This will help to improve the level of understanding of the risks inherent in reliance on key suppliers and enable firms to take mitigating action where appropriate;

d) Improving security arrangements, particularly concerning background checks on personnel.

How quickly can the sector recover from major operational disruption?

Individual participants report that they can recover *wholesale payments, trade clearing* and *settlement* rapidly following *major operational disruption*. The bulk of the critical financial infrastructure can be recovered within just two hours of invocation of plans. Within four hours, *core firms* can recover an average of 60-80% of normal volumes and values for *wholesale payments, trade clearing* and *settlement*.

The pattern for resumption of *trading* is, understandably, more of a gradual recovery, where less than half of participants can recover to 80-100% of normal *trading* volumes by the next working day. We view this as a commercial decision. In contrast, most *core firms* can restore 80-100% of normal *retail payment* volumes by the next working day.

These rapid recovery statistics reflect the strong commercial drivers for participants to recover *critical business functions* quickly. The results have, however, highlighted a few *core firms* which are outliers and we intend to follow up with these firms to explore the reasons behind this.

Proposed action:

In order to provide more clarity and transparency, we are proposing that we publish informal recovery time targets for restoration of *wholesale payments, trade clearing* and *settlement*. These targets would only be applicable to *core firms* and *financial infrastructure providers*. We do not expect these targets to be translated into rules and guidance – they will simply reflect observed sound practice and provide firms with concrete goals to plan for and test against.

The data suggest that reasonable target ranges for the recovery of *wholesale payments, trade clearing* and *settlement* would be **60-80% of normal values and volumes within four hours**, rising to **80-100% by the next working day**. The overall aim within these targets would be to complete material pending transactions on the scheduled *settlement* date. We are not proposing recovery time targets for other *critical business functions* but welcome the industry's feedback on whether this would be helpful.

We will also follow up with *core firms* which appear to be outliers to explore the reasons for this.

Do firms plan and prepare effectively?

Although individual recovery times are impressive, the survey indicated several areas where firms could strengthen their wider business continuity arrangements and so reinforce their collective ability to recover *critical business functions* after a *major operational disruption*. These points fall into two main categories:

a) *Business continuity plans* and testing regimes need to give more consideration to the full implications of *major operational disruption*

The vast majority of respondents report that their plans cater for *major operational disruption* but the survey indicated that these plans can be insular in nature. They need to give greater consideration to how such events could affect third parties, such as other counterparties, suppliers and neighbouring offices – and how events affecting third parties might affect the firm. Firms need to broaden the scope of their testing to consider these matters and also need to address some of the gaps we have identified in *business continuity planning* and IT testing. Firms and their suppliers also need to be more transparent and open about sharing information. Currently, many plans and testing regimes contain untested assumptions which may give firms false levels of confidence in their ability to meet targets for recovery of business functions. Firms also need to ensure that their business continuity personnel have sufficient knowledge of the business functions that their plans are supporting.

b) *Crisis management* arrangements need to be strengthened – particularly in relation to staff

The safety and well-being of staff during a crisis is paramount. Firms' plans recognise this but it is clear that there is considerable variation across participants. For example, only half of participants have plans for handling casualties (and of these, only half have been tested) and more than half of plans do not include instructions for handling fatalities. While we recognise that handling casualties and fatalities is primarily the responsibility of the emergency services, firms should ensure that their plans and testing regimes reflect how they will interact with the emergency services. Firms also need to make sure that their *crisis management* teams are sufficiently empowered with clear and approved spending powers in a crisis. In summary, most firms have the basic building blocks of *crisis management* in place but need to improve the practical application of their strategies and plans to ensure they are equipped to deal with the range of real-life situations that they may have to face. All recovery arrangements (whether technological or not) will rely upon staff in the short and long term, and plans and tests must reflect this. Firms which make these changes could strengthen their capacity to respond to crises and so improve their ability to recover *critical business functions*. Rigorous testing will help firms to achieve this.

Proposed action

We are recommending that firms should: i) broaden the scope of testing to embrace key third parties such as suppliers and counterparties; and ii) perform realistic testing of *crisis management* plans, in particular how they cover the interests of staff. Actions for the *Tripartite Authorities* as part of our follow-up project will include: building the detailed findings from the benchmarking results into the FSA's existing business continuity risk matrix (http://www.fsc.gov.uk/secure/upload/public/attachments/6/fsaBCMpaper200209.pdf) so that it becomes a reference document of sound practices; and following up findings with individual participants.

Are there any dependencies or concentrations that could be potential areas of vulnerability?

The project looked at geographical concentration and potential single points of failure across key suppliers and counterparties. The results point to five main types of concentration as follows.

a) Geographical concentration

There is a heavy concentration of primary and *recovery sites* in London. Participants reported nearly 400 critical sites (i.e. primary and *recovery sites*) of which around half are located in London within a 10km radius of Bank Junction (i.e. across a maximum distance of 20km) and of these, three quarters are within a 5km radius of Bank Junction. This was to be expected but nevertheless represents a significant level of concentration. Observed sound practice is to have recovery facilities close by (to handle day-to-day interruptions) and alternative recovery facilities further away which are not exposed to the same risks as the *recovery site*. We recognise that there are cost implications but also note that relatively few firms have alternative recovery facilities for all critical functions. That said, we understand from our discussions with firms and *recovery service providers* that there is already momentum in this area, with more London-based firms seeking alternative recovery facilities outside the M25.

We do not propose at this stage to suggest minimum distance criteria for the location of *recovery sites* as we need to look into this issue more closely before deciding whether or not to recommend a particular course of action. For example, some firms mitigate geographical concentration risk by being able to switch their business to other offices with minimal disruption.

Proposed action:

We intend to follow up geographical concentration as part of our follow-up project, for example by exploring the extent to which *core firms* and *financial infrastructure providers* are able to switch their business overseas or to offices that are unlikely to be concurrently affected. We can then form a view on whether minimum distance criteria might be a helpful yardstick.

b) Financial infrastructure providers

Another area of concentration is on *financial infrastructure providers*. These are critical to the market's ability to continue to operate and there is very little substitutability between them. This discussion paper explores some of the ways in which firms and *financial infrastructure providers* can work together to improve their collective *resilience*, regardless of the concentration that is inherent in the system. For example, *financial infrastructure providers* are willing to engage in joint end-to-end testing with firms but find that most firms do not take them up on this offer. Also, firms have widely differing assumptions about *financial infrastructure providers*' capacity to respond effectively (including alternative recovery methods and workarounds) following *major operational disruption* which might distort the timeframe for their own planned recovery.

Proposed action:

We are recommending that firms and their suppliers work together to increase transparency over information and join up with key providers on testing. We are proposing that new or existing industry focus groups could take this work forward with the help of the *Tripartite Authorities*.

c) Recovery service provision

The survey has revealed a low level of reliance on *recovery service providers* among *core firms* and *financial infrastructure providers* for recovery of critical IT functions. However, participant firms rely heavily on *recovery service providers* for work area recovery, be it dedicated or syndicated space. As recovery service provision was not a main focus for the benchmarking study, we are unable to comment on whether this concentration presents a bottleneck in the system – this is another potential area for future work. That said, it is clear that the lack of transparency over information on syndicated work area recovery is causing unnecessary confusion about how arrangements might be affected by multiple invocations. *Recovery service providers* accept that they need to be more proactive and open in sharing information but firms also need to improve their understanding and risk management surrounding their recovery service arrangements.

Proposed action:

As part of the follow-up project, we will work with new and existing industry focus groups and *recovery service providers* to encourage more transparency over their services. We will promote sound practice that firms can follow to improve their understanding and risk management of their third party recovery facilities. We may also include a specific survey on recovery service provision in future benchmarking exercises.

d) Information technology

Responses to the survey confirmed that participant firms are heavily reliant on information technology. Many firms operate world-class IT continuity solutions which, overall, provide a high degree of confidence that technology could be restored quickly in the event of disruption. There remain, however, several gaps that need to be addressed in planning and testing regimes which are set out in Chapter 4.

Proposed action:

We will include further information on IT sound practice when we publish our Sound Practice Guide next year. We will also encourage firms who were relatively stronger than their peers on IT continuity to share good practice with other firms, for example by speaking at business continuity seminars.

e) Telecommunications

The results confirmed our understanding that there is a significant reliance on British Telecom as a provider of voice communications. However, telecoms *resilience* must remain a focus for firms despite the Public Switched Telephone Network (PSTN) being highly *resilient* when connected to in line with the NISCC Good Practice Guide (see proposed action below and the 2005 Telecoms Resilience Assessment issued by HM Treasury at http://www.fsc.gov.uk/secure/login.asp). However, the results suggest that there is considerable scope for firms to improve their knowledge of the *resilience* of their critical telecommunications systems. For example, only 28 participants undertake full testing of their critical voice and data communications capability, nearly half of participants perform only ad hoc or no verification of the *resilience* of their telecom providers' network architectures and less than half actively plan to verify telecom providers' connectivity and routing on a regular basis, if at all. It is vital that firms understand the degree of their *dependencey* on telecoms and the *resilience* of their critical telecoms systems.

Proposed action:

We recommend that firms follow the NISCC Good Practice Guide which sets out a series of recommendations aimed at helping organisations to understand the *resilience* of their telecommunications systems. This guide can be found at http://www.niscc.gov.uk/niscc/docs/re-20040501-00393.pdf?lang=en.

2 How resilient is the UK financial sector in the face of major operational disruption?

The results indicate that individual participants have highly *resilient* IT systems, in particular the *core firms* and *financial infrastructure providers*, where three quarters of them replicate all their transactions across dual, fully staffed sites. This is encouraging but firms can do more to collaborate more closely with third parties and so strengthen the collective *resilience* of the system. Most of the detailed points relating to *resilience* are covered elsewhere in this paper and so are not repeated here. The actions needed to improve *resilience* fall into four main areas:

a) **Taking more account of key interdependencies during planning and testing (see Chapter 4)**. For example, firms could co-ordinate more closely with key third parties such as suppliers, counterparties and emergency services so that they better understand how these will behave during *major operational disruption* and in turn how their actions may affect the firm;

b) **Mitigating geographical concentration risk (see Chapter 5)**, particularly if this is coupled with reliance on certain labour pools, transport systems etc;

c) **Reducing *dependency* risk (see Chapter 5).** There needs to be more transparency over sharing of information between firms and their critical suppliers. This will improve the level of understanding of the risks inherent in reliance on key suppliers and enable firms to take mitigating action where appropriate;

d) **Improving security arrangements (see below)**, particularly concerning background checks on personnel.

2.1 Security

We anticipated that firms would have robust measures in place to manage their security in order to strengthen their first line of defence. The results confirmed that this was true for many areas – for example, almost without exception, all premises are monitored by 24 hour security guarding and CCTV. On the other hand, fewer respondents require staff or visitors to wear visible identification badges, even though this is a very basic security measure.

We also expected to find stronger results around security checks on personnel given the threat of terrorism, continued concerns about fraud levels, and the increase in industrial espionage. For example, nine respondents never take up references or perform security background checks on contractors and temporary staff. Eighteen respondents never conduct security background checks on new staff or only do this on an ad hoc basis. The risks are all too apparent, and the absence of coherent policy and procedures in this area could potentially undermine the robust security measures firms may otherwise have put in place.

2.2 Discussion points

- *Although the financial system appears to be technologically resilient, are there vulnerabilities in other areas that could put it at risk?*
- *What action could the Tripartite Authorities take to help bring together the component parts of the system?*
- *How can firms strengthen their collective resilience?*

3 How quickly can the UK financial services sector recover in the event of a major operational disruption?

Wholesale payments, trade clearing and *settlement* underpin all other activities across the UK financial services sector so need to be restored as rapidly as possible following *major operational disruption* to maintain smooth and orderly markets and ensure ongoing confidence in the financial sector. Market forces are strong in these areas as firms do not want to incur costs (which can run into £millions per day) or suffer reputational risk through a failure to recover *critical business functions* quickly. This has resulted in recovery time capabilities of hours rather than days following *major operational disruption*. That said, we recognise that an event with widespread and catastrophic implications could result in markets being out of action or in go-slow mode for a longer period of time (as happened in the USA after September 11 2001).

However, there is currently a lack of information across the market about what constitutes sound practice for recovery of *critical business functions*, and several firms have indicated that they would welcome concrete targets to aim and plan for. For this reason, we are proposing to publish informal recovery time objectives for *core firms* and *financial infrastructure providers*. These targets would not apply to other firms but could be used to help inform their planning assumptions.

The data suggests that reasonable target ranges for *core firms* and *financial infrastructure providers* would be to recover 60-80% of normal values and volumes within four hours, rising to 80-100% by the next working day. The overall aim within these targets would be to complete material pending transactions on the scheduled *settlement* date. We would not envisage these targets being embedded into formal rules and guidance, although we invite feedback on how best to position any targets that we may publish.

The pattern for resumption of *trading* is understandably more of a gradual recovery with less than half of participant firms aiming to recover to 80-100% of normal *trading* volumes by the next working day. We view this as a commercial decision.

In contrast, most core firms aim to restore 80-100% of normal *retail payment* volumes by the next working day. As we asked only high level questions about *trading* and *retail payments* (for example, firms were not asked to break down *trading* activity by product), we need to treat the responses with care, so we do not propose to suggest targets for resumption of these functions.

If the industry agrees that informal recovery target objectives would be helpful, we will of course follow up with the *core firms* and *financial infrastructure providers* concerned.

The online questionnaire captured detailed information on participants' recovery time capabilities for *critical business functions* over two, four and 24 hour periods following activation of recovery plans. This chapter does not seek to cover the full detail of our findings but instead focuses on the recovery time findings for the most *critical business functions* i.e. *wholesale payments, trade clearing* and *settlement* and invites feedback on our proposed regulatory and oversight response. Detail on other surveys such as *trading* and *retail payments* will be shared with the industry as part of our Sound Practice Guide.

3.1 Financial infrastructure providers

The *financial infrastructure providers* report rapid recovery time capabilities of 80-100% of normal volumes and values within two hours of activation of their recovery plans. By the next business day, all *financial infrastructure providers* report that they can recover to business as normal. They achieve this through heavy investment in technology, typically mirroring all transactions over dual sites or by being able to switch operations to other offices. They can also clear backlogs quickly, with over half reporting that they would have no backlogs and a further quarter able to clear them within a working day. Further analysis on the *resilience* of the *financial infrastructure providers* is set out in Chapter 5.

3.2 Wholesale payments

The *wholesale payments* survey was completed by 35 firms who initiate or receive *wholesale payments*. Recovery time capabilities for *wholesale payments* are more aggressive than any other *critical business function*, not least because half of firms responding would incur costs of over £1m per day, with several standing to lose £25m per day if this function is not recovered. This puts many *BCM* budgets into perspective as, by contrast, a quarter of all respondents had an annual business continuity budget of less than £1m and a further quarter had no formal budget at all.

One in ten firms activate their *wholesale payments* contingency plans at the slightest sign of disruption, no matter how temporary, with half activating within the first two hours and all doing so within the working day. Among the *core firms*' *wholesale payments* functions, over two thirds are unable to tolerate an inoperative function for more than two hours.

The results reveal that *core firms* can restore *wholesale payments* with impressive speed following disruption. Recovery of this function is also clearly a priority for the majority of participant firms.

Of the *core firms* that completed the *wholesale payments* survey, half can recover 81-100% of their *wholesale payment* values within two hours of invoking their recovery plans. After four hours this rises to two thirds. After 24 hours all *core firms* have reached a minimum threshold of 41%-60% recovery. We converted this information into actual percentage volumes and values for the market, using market share data for each of the *core firms* (provided by the Bank of England). Their recovery capabilities translate into the following recovery rate for *wholesale payments* within two, four and 24 hour timeframes.

Wholesale payments	**Normal daily values**	**Normal daily volumes**
Within 2 hrs	55-85%	50-70%
Within 4 hrs	70-90%	55-75%
Within 24 hrs	75-95%	70-90%

Liaison with critical suppliers, including outsourced service providers is mainly informal. Half the respondents had discussed business continuity capability with their critical suppliers, but only six firms have progressed beyond discussions on the subject to a review of each others' plans or to performing joint testing.

3.3 Trade Clearing

The *trade clearing* survey was completed by a group of 34 participants. In the event of disruption, the cost of interest and charges (known as "carry-costs") varies considerably for participants if *trade clearing* fails to recover for a working day. For many firms, these carry costs can be material, exceeding £0.5m per day.

Of the *core firms* which completed this survey, over a third can recover 81-100% of their normal *trade clearing* within four hours of invoking their recovery plans. After 24 hours this rises to three quarters. We converted this data into actual percentage volumes and values for the market, using market share data for each of the *core firms*. Their recovery capabilities translate into the following recovery rate for *trade clearing* within two, four and 24 hour timeframes.

Trade Clearing	Normal daily values	Normal daily volumes
Within 2 hrs	20-40%	15-35%
Within 4 hrs	55-75%	55-75%
Within 24 hrs	75-95%	75-95%

Trade clearing relies heavily on third parties, but despite this heavy reliance, firms typically have little dialogue with the clearing houses about joint recovery arrangements. A third have not verified their critical clearing suppliers' business continuity arrangements, three quarters of *trade clearing* functions do not have continuity plans integrated with those of their primary clearing house, and no participants perform joint testing with their clearing house.

Firms involved in *trade clearing* reported more third party *dependencies* than other *critical business functions*. For example outsourcing was more prevalent here, with half of the 34 respondents outsourcing some or all of the *trade clearing* function.

3.4 Settlement

The *settlement* survey was completed by more firms than any other *critical business function*, 42 in total, including all of the *core firms* which account for the majority of *settlement* activity. *Settlement* is less time-critical than most of the *critical business functions* reviewed, with only nine firms activating contingency plans within four hours of a disruption affecting *settlements*, rising to 34 within a working day. Nevertheless, half of firms would expect to incur carry-costs exceeding £0.5m if *settlements* did not recover within a working day, so it is still considered an important area for recovery.

Of the *core firms* which completed the *settlements* survey, a third can recover 81-100% of their normal values within two hours of activating their recovery plans. After four hours this rises to over a half; after 24 hours to almost three quarters. We converted this data into actual percentage volumes and values for the market, using market share data for each of the *core firms*. Their recovery capabilities translate into the following recovery rate for *settlement* within two, four and 24 hour timeframes.

Settlement	Normal daily values	Normal daily volumes
Within 2 hrs	30-50%	20-40%
Within 4 hrs	45-65%	40-60%
Within 24 hrs	65-85%	60-80%

3.5 Discussion points

- *Would it be helpful to publish recovery-time targets for wholesale payments, trade clearing and settlement?*
- *If so, would 60-80% of normal values and volumes within four hours, rising to 80-100% by the next working day, be reasonable recovery targets?*
- *If we decide to publish targets, should these apply to core firms and financial infrastructure providers only, or should they apply more widely?*
- *Should we consider setting targets for other functions such as resumption of trading and retail payments?*
- *If we were to publish targets, should these be informal in nature or should they be embedded into rules and guidance?*

4 Do firms plan and prepare effectively?

Although individual recovery times are impressive (see Chapter 3), the survey indicated several areas where firms could strengthen their wider business continuity arrangements and so reinforce their collective ability to recover *critical business functions* after a *major operational disruption*. These points fall into two main categories:

a) *Business continuity plans* and testing regimes need to give more consideration to the full implications of *major operational disruption*

The vast majority of respondents report that their plans cater for *major operational disruption* but the survey indicated that these plans can be insular in nature. They need to give greater consideration to how such events could affect third parties such as other counterparties, suppliers and neighbouring offices – and how events affecting third parties might affect the firm. Firms need to broaden the scope of their testing to consider these matters and also need to address some of the gaps we have identified in *business continuity planning* and IT testing. Firms and their suppliers also need to be more transparent and open about sharing information. Currently, many plans and testing regimes are being based on assumption rather than fact which may give firms false levels of confidence in their ability to meet targets for recovery of business functions. Firms also need to ensure that their business continuity personnel have sufficient knowledge of the business functions that their plans are supporting.

b) *Crisis management* arrangements need to be strengthened, in particular concerning staff.

The safety and well-being of staff during a crisis is paramount. Firms' plans recognise this but it is clear that there is considerable variation across participants. For example, only half of participants have plans for handling casualties (and of these, only half have been tested) and more than half of plans do not include instructions for handling fatalities. While we recognise that handling casualties and fatalities is the responsibility of the emergency services, firms should ensure that their plans and testing regimes reflect how they will interact with the emergency services. Firms also need to make sure that their *crisis*

management teams are sufficiently empowered, with clear and approved spending powers in a crisis. In summary, most firms have the basic building blocks of *crisis management* in place but need to improve their practical application of their strategies and their plans to ensure they are equipped to deal with the range of real-life situations that they may have to face. All recovery arrangements (whether technological or not) will rely upon staff in the short and long term and plans and tests must reflect this. Firms which make these changes could strengthen their capacity to respond to crises and so improve their ability to recover *critical business functions*. Rigorous testing will help firms to achieve this.

4.1 Planning and testing for major operational disruption

Firms are generally confident about their core *business continuity management* capability. When asked to rate the adequacy of their business continuity strategy, three quarters of respondents believed their strategy was good or excellent, and only one felt it was poor. That said, several participants have described the benchmarking exercise as a 'wake up call' in terms of improving business continuity teams' understanding of their firms' *critical business functions*. This is a welcome development but highlights that firms need to do more to ensure that business continuity staff are sufficiently aware of the business functions they are supporting.

Sound business impact analysis is the foundation of *business continuity management* and yet the survey indicates that only half of respondents have current business impact analyses in place. We also identified room for improvement over co-ordination of planning within firms. The most common approach to *business continuity planning* is for firms to have a centralised plan written by the *business continuity management* team with supporting plans written by centralised business teams. However, a significant minority of respondents' plans are decentralised and written and owned entirely by local areas. Where there is little or no central co-ordination, there is a real risk that inconsistencies and lack of integration in planning may undermine or even jeopardise firms' success in the event of a real crisis.

One of the major findings of the exercise was a lack of integration of continuity arrangements between firms and third party suppliers. This includes outsourcing providers, key suppliers, exchanges, clearing houses, connectivity providers and *trading* counterparties. Detailed planning and coordination with external agencies (such as the emergency services and local authorities) is an area where firms can make significant improvement. Even amongst those firms that appear to be 'joined up' internally, their overall plans tend to be insular in nature, and should consider and test more carefully how disruptive events could affect third parties. For example:

- for *critical business functions* such as *trade clearing* and *settlement*, over a third of firms have had no discussions with their critical providers over business continuity and only one respondent had undertaken any form of joint testing;
- over three quarters of respondents have not involved neighbouring businesses in their *BCP* testing;
- over half of respondents have not involved the emergency services in their *BCP* testing; and
- 24 respondents report that their plans take no account of local authority emergency plans.

An isolated approach could give firms false levels of confidence in their ability to meet targets for recovering business functions if, for example, external factors prevent them from being able to deploy staff to *recovery sites* within the projected timescale. There is also a wide discrepancy in firms' understanding of what they can expect from *financial infrastructure providers*. This means that many plans are currently based on assumption rather than fact.

4.2 Crisis management – general

The formal structures and documentation needed to invoke business continuity plans and deal with the aftermath of an incident are well embedded in firms. That said, it is clear from some of the responses that the quality and efficacy of these arrangements could be improved.

Nearly three quarters of participants said that they have in place a formal *crisis management* structure with clearly defined roles and responsibilities, the rest reporting that they have more informal arrangements. Fifty participants reported that they have a detailed written *crisis management* plan.

Core *crisis management* teams tend to be larger and potentially more unwieldy than might be expected, with half of them having ten or more members. Over a third of *crisis management* teams either do not have designated deputies or have not involved deputies in testing. Both of these points call into question firms' abilities to react swiftly in a crisis. Delays in contacting key individuals, particularly in the absence of trained deputies, may impinge on their firm's ability to respond effectively. In addition, the larger the team the more likely it is they will experience such difficulties. *Crisis management* teams should therefore guard against size becoming an obstacle to effective communication and decision making.

A quarter of respondents do not continuously review or adjust the composition of their *crisis management* team in line with changing threats. Keeping this under review will increase flexibility and ensure that firms take into account changes in potential threats and states of alert.

We also noted scope for improvement over the remit of *crisis management* teams. For example, a quarter of firms' *crisis management* teams are not empowered to make all necessary decisions on their firm's behalf. This lack of empowerment could lead to delays in responding to a crisis, and other responses suggest that, even where the teams are empowered, that level of empowerment is not clearly understood.

Twenty six of the 62 respondents indicated that their *crisis management* teams have clear and pre-approved spending powers during a crisis. Thirty do not have clear and pre-approved spending powers and six firms have no spending power at all. The implication is that *crisis management* teams could have significant constraints on their ability to take swift and decisive action.

Nearly all respondents have proven their *crisis management* capabilities through minor incidents. This provides some reassurance that their procedures have been shown to work. Testing regimes (as we note above) do not appear to give sufficient consideration to the full implications of *major operational disruption* and the resultant chaos that can ensue. Firms should be designing testing regimes that operate outside their comfort zones and which reveal areas of weakness rather than simply reinforcing what they do well.

4.3 Crisis management – staff

Whilst firms appear to invest in the tangible infrastructure components of continuity there is considerably less certainty around the functioning and welfare of their people in a crisis. For example, they may be suffering from shock and unable to work at the levels required, which may delay recovery and have implications for the level of resource needed following invocation of contingency plans.

All but three respondents reported that they have a human resources strategy that supports business continuity. While on the face of it firms appear to be adhering to best practice, their good intentions could be undermined by a lack of robust strategies and structures. Responses indicated that firms could improve their plans by a more thorough understanding of emergency services' procedures, staff training, and realistic planning of how a genuine crisis situation could unfold. A need for improvement around people issues is demonstrated throughout participants' responses. For example:

- more than half of participants do not address the issue of staff fatalities in their plans;
- only half of respondents said they have plans for handling casualties but only half of these have been tested;
- 12 firms do not have next-of-kin data available to provide to the emergency services on evacuation, which could lead to serious and embarrassing delays in contacting the relatives of casualties following a major incident;
- 13 respondents have not planned for severe travel disruption;
- just over a third of respondents claimed that their staff would not be affected by travel disruption following a *major operational disruption*;
- a quarter of respondents' plans take no account of where staff live or how they travel into work. Another quarter acknowledge this problem but make no specific provision, and only a quarter make limited provision for the transportation of staff;
- just over half of respondents would expect their staff to be able to operate from alternate sites for extended periods of time, but have not consulted their staff on whether this is feasible and so have no evidence of whether this will work in practice;
- 43 respondents do not have policies preventing key staff from travelling together. The impact of a major disruptive event could be compounded if groups of key individuals were affected by the same incident; and
- 25 firms recognise they may need to employ temporary staff following a major incident, but have no plans for how they would go about recruitment or deployment.

Training is another potential area for improvement. Only 42 firms include *business continuity planning* in induction programmes for new staff, and ten respondents had provided training to less than 5% of their staff. Fewer than a third of participants have provided training to staff that might be called upon to deal with sensitive issues, such as working on a casualty helpline. The responses to these and a number of other questions indicate a lack of appropriate training needs analysis and a need for greater consideration of the effects of a crisis on those who might be asked to undertake some of the most harrowing and disturbing roles.

Forty firms have a *business continuity plan* dependent on some form of external specialist support although 24 of these do not involve these third parties in exercises. In the event of a *major operational disruption* affecting many organisations, the ability of these external providers to service all of their clients' needs under such circumstances is unproven.

In summary, survey responses relating to *crisis management* and human resources show that most firms have the basic building blocks in place, but they have not tackled the more complex aspects of human interaction which only reveal themselves in realistic testing or genuine incidents. All recovery arrangements (whether technological or not) will rely upon staff in the short and long term and plans and tests must reflect this. Firms therefore need to strengthen their *crisis management* arrangements, in particular paying greater attention to the interests of their staff.

The *Tripartite Authorities* can also play a role by acting as a catalyst for more coordination across the sector, encouraging more joined-up testing, and sharing information. We also intend to follow up findings from the benchmarking exercise with individual firms as part of our ongoing supervision and oversight work.

4.4 Discussion points

- ***What more can be done to encourage joined-up planning and testing to reflect better the likely impact of a major operational disruption and how this could be facilitated?***
- ***Could the weaknesses in business continuity and crisis management arrangements undermine recovery time capabilities?***

5 Are there any dependencies or concentrations that could be potential areas of vulnerability?

The project looked at geographical concentration and potential single points of failure across key suppliers and counterparties. The results point to five main areas of concentration as follows.

5.1 Geographical concentration

There is a heavy concentration of primary and *recovery sites* in London. This was not unexpected but nevertheless represents a significant level of concentration. For example:

- participants reported nearly 400 critical sites (i.e. primary and *recovery sites*), of which around half are located in London within a 10km radius of Bank Junction (i.e. across a maximum distance of 20km). Of these, three quarters are within a 5km radius of Bank Junction; and

- of the *core firms* and *financial infrastructure providers*, two thirds have their primary offices and recovery sites in inner London, over half of which are less than 10km apart. Of these, half are less than 5km apart.

The significant level of concentration in London is a potential area for concern, particularly where this applies to the *core firms* and *financial infrastructure providers* who have the highest responsibility to develop *resilient* arrangements. That said, several *core firms* operate either from multiple locations or from out-of-town, and a third of all participants report that they perform their *critical business functions* outside of London. Against this background it is perhaps slightly less surprising to discover that over a third of all respondents believe they would not be affected directly by a London-based scenario.

We also know that some of the organisations that are subject to the London concentration risk have the facility to switch many of their *critical business functions* overseas or to regional offices – indeed we have found that a number of them do so routinely in the normal course of business. This gives us greater confidence in their *resilience* and recovery capability in the event that both their London primary offices and *recovery sites* were affected by an event. Nonetheless this is an issue we intend to explore in greater detail as part of our follow-up project.

Sound practice is to have a *recovery site* close by (to handle day-to-day interruptions) and alternative recovery facilities further away which are less exposed to the same risks as the main *recovery site*. We recognise that there are cost implications but also note that relatively few firms have alternative recovery facilities for all functions. That said, we understand from our discussions with firms and *recovery service providers* that there is already momentum in this area, with more London-based firms seeking alternative back up facilities outside the M25.

We do not propose at this stage to suggest minimum distance criteria for the location of *recovery sites* as we need to look into this issue more closely before recommending a course of action. For example, some firms mitigate geographical concentration risk by being able to switch their business to other offices with minimal disruption. There are also other factors to consider such as the extent to which *recovery sites* are located in discrete risk environments – distance alone does not necessarily mitigate geographical concentration risk.

5.2 Financial infrastructure providers

Another area of concentration is on *financial infrastructure providers*. These are critical to the market's ability to continue to operate and there is very little substitutability between them. This section explores some of the ways in which firms and *financial infrastructure providers* can work together to improve their collective *resilience*, regardless of the concentration that is inherent in the system.

Overall, the recovery claims for the *financial infrastructure providers* are impressive and should give comfort to market participants that disruption to the underlying markets due to financial infrastructure failures would be minimised. Nonetheless, there are still risks to be considered. For example, *financial infrastructure providers* need to improve their understanding of the recovery times of those organisations on which they are dependent. For example, they gave a range of answers on how quickly they expect their key suppliers such as information providers to restore services following disruption.

Financial infrastructure providers have taken operational steps to strengthen their *resilience* and recovery and mitigate the risks arising from activity concentration, in most cases via distributed 'live-live' computer architectures and staff skills duplication. Over half have staff permanently manning their recovery/alternative site, a source of *resilience* given the points raised in this paper and elsewhere about the 'people' consequences of a disruption, including the ability of staff to travel. *Financial infrastructure providers* rely on a high level of IT automation but to mitigate this risk they have invested heavily in *resilient* IT systems. This degree of *resilience* and automation leads to considerable confidence among the *financial infrastructure providers* in their ability to continue operating, to the extent that they report little reliance on staff to continue operating, at least in the short term.

Financial infrastructure providers appear willing to engage in end-to-end joint testing, but the take-up for this is low. Firms and *financial infrastructure providers* could work more closely to understand their respective requirements and engage, where appropriate, in joint testing of *business continuity plans*. Whilst taking the entire system down for tests may be unrealistic, the effects of concurrent cutover should be known.

Despite this, *core firms* are more *resilient* to the failure of a *financial infrastructure provider* than might actually be expected because of their diversity (for example their ability to switch *trading* to a different exchange, or make payments via an alternative payment network). This substitutability is key, although the reality remains that the failure of any of the *financial infrastructure providers* to operate would have a substantial effect on the market overall.

That said, the *financial infrastructure providers'* impressive, well-proven, and documented recovery capabilities provide a strong foundation for market recovery, and should form the basis on which firms build their own recovery plans. Firms, however, have widely differing assumptions about *financial infrastructure providers*' functionality (including alternative recovery methods and workarounds) following *major operational disruption* which might distort the timeframe for their own planned recovery. They should try to to obtain accurate, up-to-date statements of recovery timeframes from all of their critical suppliers to ensure that overall planning assumptions are valid and consistent. Failure to do so may delay the market's ability to recover in the event of a disruption.

5.3 Recovery service provision

The survey has revealed a reassuringly low level of reliance on *recovery service providers* among *core firms* and *financial infrastructure providers* for recovery of critical IT functions. However, participant firms rely heavily on *recovery service providers* for work area recovery, be it dedicated or syndicated space. As recovery service provision was not a main focus for the benchmarking study, we are unable to comment on whether this concentration presents a bottleneck in the system – this is another potential area for future work. That said, it is clear that the lack of transparency over information on syndicated work area recovery is causing confusion and conjecture about how arrangements might be affected by multiple invocations. *Recovery service providers* accept that they need to be more proactive and open in sharing information but firms also need to improve their understanding and risk management surrounding their recovery service arrangements.

Forty two of the 62 participant firms have work area recovery facilities with third party providers. The others have either dedicated space or a mix of shared and dedicated facilities. In total (UK wide), participant firms have purchased nearly 12,000 syndicated work area recovery seats and 4,000 dedicated seats from third party providers. There is therefore considerable use of third party facilities and hence interest across the sector around recovery service provision, particularly the extent to which syndicated work area recovery seats would be available in the event of multiple invocation.

As recovery service provision was not a main focus of the benchmarking study, we are not able to comment on matters such as syndication ratios and exclusion zone policy as we did not ask detailed questions about this topic. That said, we met the main *recovery service providers*, both individually and collectively, to discuss their policies relating to space allocation, and to establish how they might address the concerns that firms raised with us during the course of the project.

These meetings revealed two main disconnects. The first issue was raised by firms. They would welcome more transparency and openness from suppliers on matters such as syndication ratios, exclusion zones, and the number of other clients which have purchased the same seats. *Recovery service providers* were surprised to hear this as (bearing in mind the need to protect the identity of other clients) they state that they have always been willing to share this information. They accepted, however, that they needed to be more proactive in getting these messages across.

The second point was raised by *recovery service providers*, who were concerned that their clients could do more to understand and manage their risks surrounding recovery space. For example, firms' senior management need to understand the risks inherent in purchasing syndicated space. They could do this by seeking an annual risk statement from their supplier setting out how

their risk profile might have changed since the previous year, including whether syndication ratios for the seats they have bought have increased or fallen. Firms should also ensure that they regularly test their recovery facilities – many do not test regularly despite this being allowed for in their contracts.

The Business Continuity Institute has recently issued a transparency guide for recovery service provision which firms may find helpful as tool to address many of the points that we raise above. This guide is replicated at Annex E and can be found on the BCI website at http://www.thebci.org/.

We also propose to follow up in more detail on recovery service provision as part of our new project, possibly by including a specific survey on this issue in future versions of the online questionnaire. This is an area where we will continue to encourage more transparency over information sharing, including sharing sound practice.

5.4 Information technology

Responses to the survey confirmed that participant firms are heavily reliant on information technology. Many firms operate world-class IT continuity solutions which, overall, provide a high degree of confidence that technology could be restored quickly in the event of disruption. However, there remain several gaps that need to be addressed in planning and testing regimes. For example:

- only half the respondents knew how long it would take to recover each of their critical systems;
- only 11 perform testing during business hours and eight participants have not tested mirrored systems with the primary system turned off;
- 17 participants do not have a policy that includes testing outsource suppliers' disaster recovery capabilities; and
- 12 participants have not tested critical backup tapes in the last six months.

IT is a critical factor in firms' *resilience* and recovery capabilities. More comprehensive planning and testing would lead to even greater confidence in firms' abilities in this area.

5.5 Telecommunications

The results confirmed our understanding that there is a significant reliance on British Telecom as a provider of voice communications. However, telecoms *resilience* must remain a focus for firms despite the Public Switched Telephone Network (PSTN) being highly *resilient* when connected to in line with the NISCC Good Practice Guide (see proposed action in Chapter 6, and the 2005

Telecoms Resilience Assessment issued by HM Treasury and published at http://www.fsc.gov.uk/secure/login.asp). However, the results suggest that there is considerable scope for firms to improve their knowledge of the *resilience* of their critical telecommunications systems. For example, only 28 participants undertake full testing of their critical voice and data communications capability, nearly half of participants perform only ad hoc or no verification of the *resilience* of their telecom providers' network architectures and less than half actively plan to verify telecom providers' connectivity and routing on a regular basis, if at all. Similarly, only around a third of respondents said their telecom providers were mostly, or always, proactive in passing on information about risk. It is vital that firms understand the degree of their *dependency* on telecoms and the *resilience* of their critical telecoms systems.

Given the high degree of reliance on telecoms and voice services, it is clear that firms and suppliers need to work more closely to improve understanding and perform more effective testing of telecoms and voice services. The *Tripartite Authorities* will continue to act as a catalyst in this area, for example by encouraging providers and firms to share information on sound practice and promoting the use of the NISCC Good Practice Guide on Telecoms Resilience which can be found at http://www.niscc.gov.uk/niscc/docs/re-20040501-00393.pdf?lang=en.

5.6 Discussion points

- ***Would it be helpful to set a minimum distance criteria between primary and recovery sites? If so, what should that distance be?***
- ***Should we actively encourage firms to diversify their back-up arrangements, in particular core firms and financial infrastructure providers?***
- ***Do you agree with our conclusions and proposed actions in relation to recovery service provision? Is there more that the Tripartite Authorities should do in this area – for example including a specific survey on recovery service provision in future benchmarking studies?***
- ***We invite feedback on the measures we propose to take to mitigate concentration risk: encouraging end-to-end testing; sharing information on resilience and recovery arrangements the financial infrastructure providers have in place; and encouraging wider geographical diversification.***

6 What action is needed to improve the resilience and recovery capability of the sector?

The following table summarises the actions we are proposing for the *Tripartite Authorities* and for firms. Annex A considers the cost and benefits of these proposed actions and seeks feedback on discussion points raised.

ACTIONS FOR THE *TRIPARTITE AUTHORITIES*
Seek feedback on whether we should publish informal recovery time targets for restoration of *wholesale payments, trade clearing* and *settlement* by *core firms* and *financial infrastructure providers*.
Build the detailed findings from the benchmarking results into the FSA's existing business continuity risk matrix so that it becomes a reference document of sound practices.
Follow up the results of the benchmarking exercise through a new project which will include co-ordinating the follow-up work for individual participants and looking more closely at issues arising from geographical concentration and *recovery service provision*.
Follow up with individual participant firms on their benchmarking results as part of our supervision and oversight arrangements.
Lay the foundation and put in place incentives to encourage market participants to develop more integrated testing plans including recovery of links to key third parties. This could include themed seminars involving financial sector participants.
Encourage *financial infrastructure providers* and *recovery service providers* to increase transparency over their services.
Build on our understanding of how different disruptive scenarios will affect the financial system and develop sector-wide strategies for dealing with these.
Analyse findings and use these as a catalyst for work in other areas e.g. over utilities, telecoms, power etc.
Repeat the formal benchmarking exercise for *core firms* and *financial infrastructure providers* in around 18 months – and in future years possibly use the average benchmarks from this year's exercise to encourage continuous improvement.
Roll out a simplified version of the benchmarking questionnaire to a wider group of firms.
Use the benchmarking exercise results to influence future Market Wide Exercises

ACTIONS FOR FIRMS
Participant firms to review benchmarking results and strengthen relative and absolute weaknesses.
Broaden the scope of plans and testing to include key third parties such as suppliers, counterparties, emergency services, local authorities and infrastructure providers.
Perform realistic testing of *crisis management plans*, in particular how they cover the interests of staff.
Work more closely with suppliers to increase transparency over information.
Reconsider the potential practical implications of a *major operational disruption* e.g. travel disruption, casualties and fatalities, and the psychological impact on staff.
Take steps to mitigate concentration risk (and its potential impact).
Follow the NISCC Good Practice Guide which sets out a series of recommendations aimed at helping organisations to understand the *resilience* of their telecommunications systems.

Cost Benefit Considerations

Introduction

This discussion paper describes the headline findings of the Resilience Benchmarking Project and sets out what action is needed to improve the *resilience* and recovery capability of the financial sector. The results do not suggest that we need to be more prescriptive in our approach to *business continuity management* and therefore we are not proposing to make any new rules or guidance at this stage. We do, however, set out various proposals for taking this strand of work forward. These include:

- publishing specific recovery targets for the *core firms* and *financial infrastructure providers*;
- encouraging greater transparency between firms and their key suppliers, promoting information sharing and more coordinated testing;
- publishing a detailed paper on observed sound practice;
- following up specific concerns in relation to individual participants; and
- using the findings as a catalyst for further work (for example, exploring in greater detail how firms mitigate geographical concentration).

This Annex sets out, at a very high level, the types of costs and benefits to market participants associated with these proposals. However, although we acknowledge that there are some market failure issues resulting from externalities and information asymmetries, we have not undertaken a full cost benefit analysis as we are not proposing any new rules or guidance.

Market failure analysis

Market failures may arise as a result of externalities and information asymmetries.

Information asymmetries exist where one group of market participants has more or better information than another group, which they can then exploit to the detriment of the other. For example, as noted (in Chapter 5 above) the lack of transparency over information on syndicated recovery space is causing unnecessary confusion and conjecture about how arrangements may be affected by multiple invocations.

Negative externalities arise where the economic decisions of one firm impose costs on another. Firms tend to only consider the cost benefit implications of the decisions they take in relation to their own businesses, which may mean that the decisions they take do not necessarily lead to the best outcomes for the financial services sector as a whole or for the wider environment in which they operate.

As we have seen elsewhere in this paper, we are recommending that firms should improve their understanding of how, in the context of a *major operational disruption*, their actions and decisions would impact on others, or how others potentially impact on them. In particular, we have identified the core market and financial infrastructure functionality on which the rest of the market is heavily dependent. In a worst case scenario, the failure of one or more of the providers of this core functionality could transmit disruption across the financial system and the impact of these negative externalities could be amplified many times over. Conversely, by strengthening the weaker links and reducing vulnerabilities, not only do individual organisations become more *resilient* but they also become better able to act as shock absorbers for the system, reducing the likelihood of transmission and therefore the impact on the sector as a whole.

In the event of a wide scale disruptive incident, the effects of such negative externalities are potentially extensive. The financial sector is a system of complex interdependencies. Firms depend on each other to the extent that they would struggle to exist in isolation from that system. As such, it is in firms' best interests not only to protect themselves but to ensure that they act in the interests of the sector as a whole so they can benefit from its collective strength.

Our proposed approach

We are mindful of the strong market forces which already exist in this area. It is in firms' own interests to ensure they have robust *resilience* and recovery arrangements. The survey demonstrated that they have strong financial incentives for doing so – for most participants the financial cost of having to suspend or curtail their normal business operations would be at least £0.5m

per day, with some firms standing to lose up to £25m per day. This puts many firms' business continuity budgets into perspective. Furthermore, firms could suffer serious reputational damage by being out of the market – particularly if this was at variance with their peers.

However, although this paper sets out numerous areas of perceived strength in the financial sector's *resilience* and recovery arrangements, there are several areas where there is scope for improvement. Because of this we consider it would be an insufficient response simply to maintain the status quo – at the very least there is clearly a need for greater coordination and information sharing across the sector. In considering how we might best address these matters we reflected on whether our current, non-prescriptive stance, remained appropriate.

Option 1 – Increase regulation: Specifically this option might include making rules and guidance, particularly in respect of the recovery target objectives proposed in Chapter 3. Our analysis indicates that, in order to maintain market stability, these recovery objectives need only apply to a small number of *core firms* and *financial infrastructure providers*. Therefore, to formalise these recovery objectives in rules and guidance would be disproportionate to the rest of the market, imposing undue costs without achieving significant tangible benefit.

The introduction of new rules and guidance would result in an increase in direct costs for the FSA, including the cost of enforcing compliance. These costs would have to be passed on to firms via their regulatory fees, increasing the cost of regulation as well as compliance costs.

Option 2 – Sharing information and sound practice: There is a strong appetite within the market for information and examples of sound practice. Equally, whilst there are elements of sound practice which are relevant to all organisations, there are some areas which are more nuanced and what is appropriate for one is not necessarily appropriate for another. As discussed above, we consider that market forces are very strong in this area, and that more regulation would not have the corresponding level of added value. Furthermore, as discussed in Chapter 5, we recognise that diversity is a key component of *resilience*, both in terms of individual firms and across the market as a whole.

For these reasons we do not propose to formalise standards within rules and guidance. Rather, we will use the benchmarking results to build on our existing good practice matrix which we will issue in the form of a Sound Practice Guide. Where we have identified specific concerns in relation to individual participants we will explore these on a firm by firm basis as part of our follow up project and, where necessary, seek remedial action. This approach is likely to have fewer cost implications for firms.

We recognise that there is a commercial balance to be struck in decisions relating to *resilience* spending, and that much of this depends on an organisation's risk appetite. At the same time, the most *resilient* organisations are those least likely to need to activate their recovery plans. Returning to the market failure analysis, firms also need to be mindful of the positive and negative impact their decisions could have on their counterparties and, in turn, the market as a whole. We feel this can best be achieved through sharing information and promoting dialogue and greater integration between firms and their key counterparties.

Conclusion

The results of the benchmarking survey do not suggest that we need to change our non-prescriptive regulatory stance on *business continuity management*, although we propose to conduct all follow up work emanating from the project in a coordinated way through a new project. However, we will need to keep this strategy under review as we monitor the market's progress towards strengthening its *resilience*.

Discussion points

- ***Should FSA maintain its non-prescriptive approach to business continuity management?***
- ***We would welcome comments on the estimated cost of reaching the targets we propose to set for core firms and financial infrastructure providers:***
  - ***from those organisations to which these targets would apply; and***
  - ***from other organisations for which these targets might be considered aspirational goals.***
- ***We would welcome views on the estimated cost of lost business arising from the delayed recovery of a vital counterparty (i.e. a core firm or infrastructure provider)***

Summary of discussion points

1 Although the financial system appears to be technologically *resilient*, are there vulnerabilities in other areas that could put it at risk?

2 What action could the *Tripartite Authorities* take to help bring together the component parts of the system?

3 How can firms strengthen their collective *resilience*?

4 Would it be helpful to publish recovery-time targets for *wholesale payments, trade clearing* and *settlement*? If so, would 60-80% of normal values and volumes within four hours, rising to 80-100% by the next working day, be reasonable recovery targets?

5 If we decide to publish targets, should these apply to *core firms* and *financial infrastructure providers* only, or should they apply more widely?

6 Should we consider publishing targets for other functions such as resumption of *trading* and *retail payments*?

7 If we were to publish targets, should these be informal in nature or should they be embedded into rules and guidance?

8 What more can be done to encourage joined-up planning and testing to reflect better the likely impact of a *major operational disruption* and how this could be facilitated?

9 Could the weaknesses in business continuity and *crisis management* arrangements undermine recovery time capabilities?

10 Would it be helpful to set a minimum distance criteria between primary and recovery sites? If so, what should that distance be?

11 Should we actively encourage firms to diversify their back-up arrangements, in particular *core firms* and *financial infrastructure providers*?

12 Do you agree with our conclusions and proposed actions in relation to recovery service provision? Is there more that the *Tripartite Authorities* should do in this area – for example including a specific survey on recovery service provision in future benchmarking studies?

13 We invite feedback on the measures we propose to take to mitigate concentration risk: encouraging end-to-end testing; sharing information on *resilience* and recovery arrangements the *financial infrastructure providers* have in place; and encouraging wider geographical diversification

14 Should FSA maintain its non-prescriptive approach to *business continuity management*?

15 We would welcome comments on the estimated cost of reaching the targets we propose to publish for *core firms* and *financial infrastructure providers*:

- from those organisations to which these targets would apply; and
- from other organisations for which these targets might be considered aspirational goals.

16 We would welcome views on the estimated cost of lost business arising from the delayed recovery of a vital counterparty (i.e. a *core firm* or *financial infrastructure provider*).

Glossary of terms

BACS – Bankers Automated Clearing System

Provides processing of bulk electronic payments (e.g. direct debits, electronic payments, and standing orders).

BCM – Business continuity management

A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building *resilience* with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

BCP – Business continuity plan

A clearly defined and documented plan for use at the time of a business continuity emergency, event, incident and/or crisis. Typically a plan will cover all the key personnel, resources, services and actions required to manage the *BCM* process.

Cashflow & liquidity

The ability of the organisation to manage and control the risks associated with market positions by ensuring that funds and *securities* are available to meet obligations and hedge risks as appropriate in the event of a *major operational disruption*.

CHAPS – Clearing House Automatic Payment System

CHAPS is the United Kingdom's high volume payments system, providing members with Real Time Gross Settlement (RTGS) of credit transfers.

Core Firms

For the purpose of this exercise, *core firms* means firms which, as part of their business, provide key market or infrastructure functionality, the failure of which could impact significantly on other firms in the market. It does not include those entities of which the main or sole function is the provision of financial infrastructure services (see *financial infrastructure providers* below). The FSA will contact all firms which we regard as *core firms* for the purpose of this exercise.

Crisis management

The process by which an organisation manages the wider impact of a business continuity emergency, event, incident or crisis until it is either under control or contained without impact to the organisation or the *BCP* is activated as part of the *crisis management* process.

Critical business functions

The operations and/or business support activities (internal or outsourced) without which the organisation would be unable to achieve its business objectives. For the purposes of this exercise, they are defined as *wholesale payments, trade clearing, securities settlement, cashflow and liquidity, trading, retail payments* and *custody*.

Custody

The holding of financial assets and *securities* in safekeeping, including the provision to clients of *settlement* and reporting services for all classes of financial instruments.

Dependency

Operations or support activities upon which a *critical business function* is dependent to enable it to fully complete.

Financial infrastructure providers

Key UK-based exchanges, clearing and *settlement* houses and payment system operators.

Major operational disruption

An incident having widespread impact on more than one organisation, that has a severe impact on firms and that requires the implementation of special arrangements for continued operation of *critical business functions*.

Recovery capacity

The time by which a *critical business function* and or any *dependencies* following a *major operational disruption* should be recovered.

Recovery service providers

Third party providers of syndicated or dedicated business or IT recovery space on a contract basis. Sometimes known as Disaster Recovery site providers.

Recovery site

A site designated to maintain continuity of *critical business functions*.

Resilience or resilient

The ability of a firm (staff, systems, network, activity or process) to absorb the impact of a major business interruption, disruption and/or loss and continue to provide a service at an acceptable level.

Retail payments

Payment received through retail banking services. This involves the initiating, clearing or receiving of *retail payment* transactions for end-customers, whether by cheque, debit and credit cards, ATM transactions and *BACS* or *CHAPS* direct transfers.

RTGS – Real time gross settlement

The continuous settlement of payments on an individual order basis without netting debits with credits across the books of a central bank.

Securities

Instruments that signify an ownership position in a corporation, a creditor relationship with a corporation or governmental body, or other rights to ownership.

Settlement

The process of transferring ownership after a trade has been carried out.

Trade clearing

Process of clearing whereby the mutual obligations of the market participants are calculated for the exchange of *securities* and cash.

Trading

The act of a buyer and seller coming together and agreeing to exchange a given *security* (or contract in the case of derivatives) at an agreed price and point in time. *Trading* can be executed via an exchange-provided *trading* system, or over the counter.

Tripartite Authorities

HM Treasury, the Bank of England and the Financial Services Authority (FSA).

Wholesale payments

Payment transactions, usually of large value and high-priority, made by corporates and financial institutions. These can include the discharging of obligations both with respect to non-financial instruments and in relation to the transfer of securities and other financial instruments in other parts of the financial infrastructure.

Our approach

This appendix supplements provides more information on the approach to the Resilience Benchmarking project. It covers:

- The role of the Industry Support Group and the consultants
- INONI™ detail and sample output
- Questionnaire development and structure

The role of the Industry Support Group and the consultants

To provide specific industry experience we established an Industry Support Group comprised of a cross section of market participants. The group was created in January 2005 and met with the project team on a monthly basis, with additional meetings as required. The group provided valuable feedback on, amongst other things:

- The overall approach to the benchmarking project
- The composition of the web-based questionnaire
- The design and development of specific scenario based questions
- The criteria for selecting participant firms

Some of the members were also involved in other industry focus groups, e.g. SIBCMG (Securities Industry Business Continuity Management Group). As a result they were able to act as a conduit for information between the groups.

The extensive consultation with the support group during the early stages of the project, especially those covering *critical business functions*, helped ensure the relevance of questions. Organisations that provided representatives for the group were:

Bank of England (*RTGS*)	*CREST*Co	LIFFE
Bank of New York	Goldman Sachs	London Stock Exchange
Bank of America	HSBC	Morgan Stanley
UBS	Legal and General	Royal Bank of Scotland

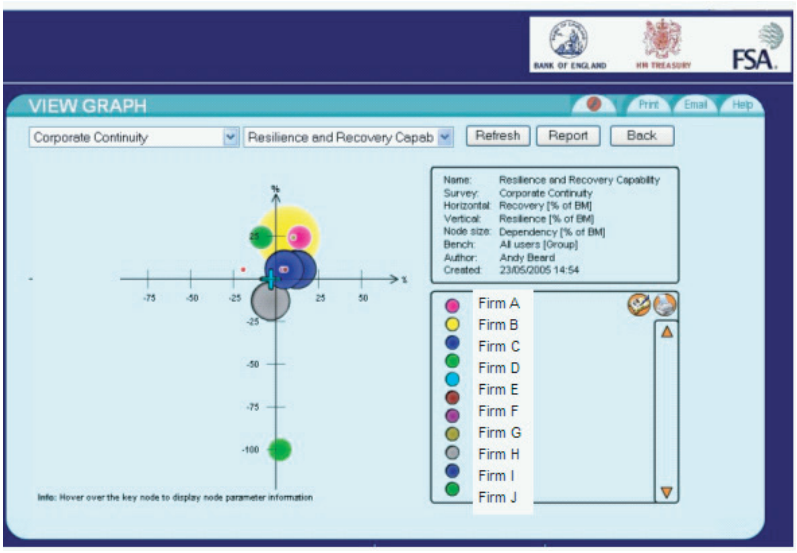
In February 2005 the FSA project appointed PricewaterhouseCoopers as external consultants to the project. They in turn subcontracted elements of the work to JR Consulting Partners Ltd who supplied the diagnostic tool (INONI™) used for collecting participants' responses and provided specialist business continuity tools with the help of Clifton Risk Management and Survive.

INONI™

Having agreed that the most effective way of collating the information would be to develop an online benchmarking questionnaire, we selected an online diagnostic tool called INONI™. INONI™ is a programmable online expert system, designed to collect and respond to the opinions or factual data supplied by users. Respondents were required to answer multiple choice questions (see Figure1).

Figure 1

INONI™'s diagnostic features have produced the individual reports that the participants have received. An example of the type of information participants have received is provided in the following diagram. These graphs provide an overview of individual firms' positions relative to their peers.

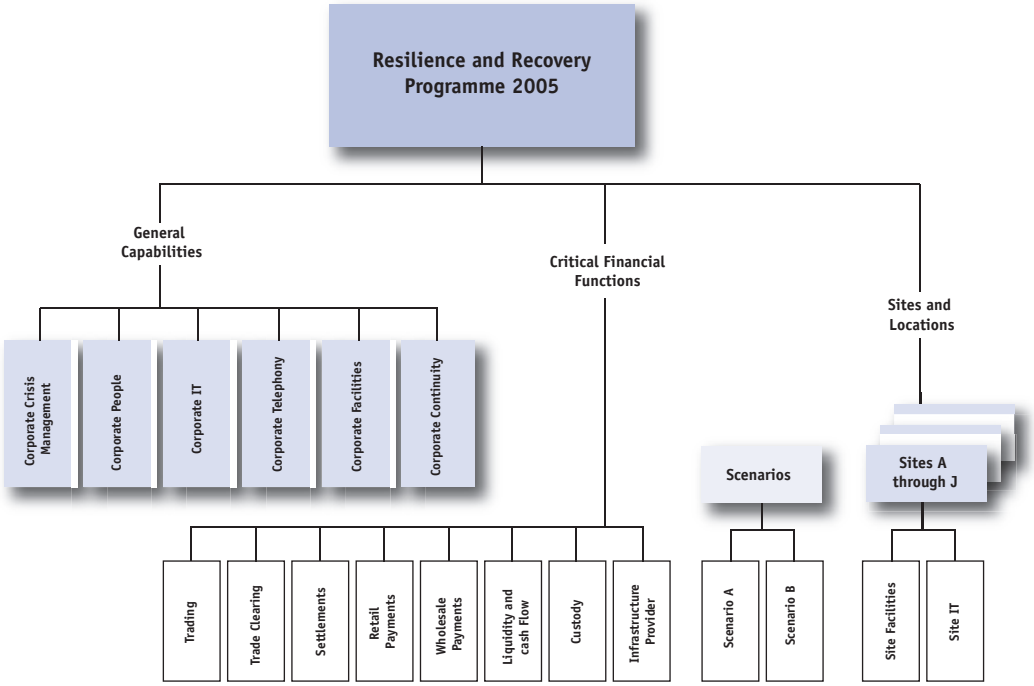


Questionnaire development and structure

The questions were developed using the combined expertise of the consultants in consultation with the FSA and the Industry Support Group. This helped ensure that the questions were sufficiently detailed to provide meaningful and verifiable information. To reflect the need to cover wide ranging continuity related disciplines the surveys were created in four broad categories:

- *Critical business functions*. In order of priority these are: completion of *wholesale payments, trade clearing, settlement* of existing trades, management of *cashflow and liquidity*, resumption of *trading*, for example to commit to new positions and meeting retail obligations e.g. customers immediate demands for cash, credit and debit transactions. (Definitions of these areas are expanded in the Glossary of terms).
- Recovery and *resilience* questions that tested whether *critical business functions* are underpinned by strong business continuity practices.
- Specific sites that firms depend on for *critical business functions*.
- Scenario-related issues to test how the participants would respond to two different disruption scenarios.

The structure of the questionnaire including individual surveys and the relationship between the categories is illustrated in the following diagram.



Validation

We validated the responses given in the questionnaire by including 'check and balance' questions in the scenario surveys which were only released to participants once they had committed their responses to the corporate surveys. Where possible, questions asked whether firms had documented procedures and so firms were on notice that we may ask to see these. We also conducted six validation visits to a selection of firms to check their responses and confirm that our approach was appropriate.

Further Information

Additional information on the project background, approach, and methodology can be found on the UK Financial Sector Continuity website at http://www.fsc.gov.uk/section.asp?catid=320&docid=942

BCI VOLUNTARY SUPPLIER RISK DECLARATION – SAMPLE COPY ONLY

Customer Name:	Abc plc		
Contract Reference:	xxxxxxx	As at:	Date
Client Site: Xxxxxxxx Xxxxxxxx Xxxxxxxx	Site: 1 of 1	Primary Recovery Site: Xxxxx Xxxxx Xxxxx Xxxxx	

We continually monitor the risk profile of services supplied to our clients. As a subscriber to our services you will receive a Voluntary Supplier Risk Declaration at commencement of your contract and an updated Declaration every subsequent year on or around your contract anniversary. This important information enables our clients to regularly evaluate the risks associated with outsourced services against their appetite for such Risks. A traffic light system has been used to highlight the service risk status and areas of potential concern. (GREEN – Acceptable, AMBER – Requires Attention, RED – Warning)

RECOVERY SITE STATUS

Recovery Centre Size:	xx,000 square feet	Site Dedicated Seats:	xx at issue date
Secure Recovery Suites:	x	Site Syndicated Seats:	xx
Workplace invocations at the centre during the last 12 months:		Site Dealing Positions:	xx
Total Number of contracted Seats Centre Utilisation (at issue date):	xxxxx xx%	Site Utilisation is calculated as a multiple of the number of syndicated seats at the site (as shown above) by the maximum syndication limit per seat (as stated below), divided by the number of contracted seats sold to all subscribing clients.	

CLIENT RISK STATUS

Risk with explanation	Supplier Statement	Current Position at Review Date
Service Basis The basis of the service you have contracted for the above Client Site.	The service is a Syndicated Service. The service is shared with other subscribers and may not be available in the event of multiple invocations.	To mitigate risk, syndicated services are provided to monitored exclusion zone & subscription rates as disclosed below
Service Allocation The method by which your contracted services are allocated if there are multiple invocations.	Syndicated Service is made available on a 'first come first served' basis whereby legitimate invocations are allocated resource in the order in which they are received (time logged).	Met throughout year, no contract exceptions.
Risk Statement The risk metric associated with the Client Site and the total number of sites supported by the supplier using the same asset or Recovery Site.	Each Client Site, based at a defined post code, is classified as a full subscriber on a 1:1 basis. The total number of these subscribers will not exceed the Syndication Rate applicable to the Service.	Subscriber Rates have been maintained during the year. Total number of risk sites supported from the recovery centre are xx
Syndication rates The number of times each item of equipment or workplace position (seat) can be sold to different Clients Sites.	Each asset may be sold up to a maximum of 25 subscribers per asset. Each subscriber will be located in an agreed exclusion zone area.	X:1 (workplace positions & PC's) X :1 (dealing facilities) X :1 (servers and peripherals)
Standard exclusion zones Distance between your sites and another Client or Clients syndicated to the same equipment or workplace position	Within 250m of the above address Within 250-500m Within 500-1000m	x other subscribers x other subscribers x other subscribers
SLAs (Service Level Agreements) Adherence to contracted SLA's	SLAs as stated in contract	Service Levels were met
Alternative Sites Alternative Recovery Centre available in the event the Primary site is unavailable and the basis of access to those sites.	Other sites may be made available on a reasonable endeavours basis only, subject to availability and outside of the Agreed SLA.	B Site x (xx seats xx miles) C Site x (xx seat xx miles) D Site x (xx seats xx miles)
Invocation Notification Making clients aware when equipment or workplace positions they have syndicated rights to have been invoked	Workplace – E-mail within 24 hours of invocation.	Standard met – issued within 24 hours
Testing Client contracts contain adequate test days for technology & staff rehearsal.	3+ days per annum minimum 6+ days per annum recommended	xx days per annum
Testing Test days are appropriately utilised	IT tests minimum Business User tests recommended	None undertaken None Undertaken

On behalf of Supplier, I warrant that the information is correct as at the date above.

Supplier Signature